REMARKS

Introduction

This Reply is in response to the Office Action of November 24, 2009. Reconsideration of this application in view of the following remarks is respectfully requested.

Subject Matter Indicated to be Allowable

Claims 1-12, 18, and 19 were allowed. Applicants hereby reserve the right to pursue the subject matter of these claims during subsequent prosecution should the present Reply not be considered to place this application in condition for allowance.

The Prior Art Rejections

In the Office Action, claims 13-17 were rejected under 35 U.S.C. §103(a) as being unpatentable over Boneh et al. U.S. Patent Publication No. 2003/0081785 in view of Deng et al. U.S. Patent No. 6,910,129. These rejections are respectfully traversed.

Claims 13-17

Claim 13 is directed to a method of signing and encrypting a message M in which an IBE private key is used to compute a commitment to a secret value and a corresponding

decommitment and in which a symmetric key that is based on the IBE private key is used to encrypt at least one of the commitment and the decommitment.

In the rejection of claim 13, it was stated that Boneh discloses "using the IBE private key (of a user) to compute, with computing equipment, a commitment to a secret value and a corresponding decommitment." Paragraphs 6 and 17 of Boneh were said to be relevant. Boneh, however, does not show or suggest using an IBE private key to compute a commitment to a secret value and a corresponding decommitment.

Paragraph 6 of Boneh describes conventional RSA public-key cryptosystems (i.e., non-IBE cryptosystems). There is nothing in paragraph 6 of Boneh relevant to a commitment to a secret value and a corresponding decommitment, let alone using an IBE private key to compute a commitment to a secret value and a corresponding decommitment.

Paragraph 17 of Boneh describes a method of generating a decryption key corresponding to an encryption key. There is nothing in paragraph 17 of Boneh relevant to a commitment to a secret value and a corresponding decommitment, let alone using an IBE private key to compute a commitment to a secret value and a corresponding decommitment.

Deng, which was said to show use of a symmetric key that is based on the IBE private key to encrypt at least one of

the commitment and the decommitment, does not make up for the fact that Boneh does not show or suggest using an IBE private key to compute a commitment to a secret value and a corresponding decommitment.

Deng has a commitment function formed "using a cryptographic one-way hash function h()" (see, col. 12, lines 23-38 of Deng). Deng does not, however, disclose using an IBE private key to compute a commitment to a secret value and a corresponding decommitment. In particular, Deng teaches that a user can "commit to an item I" by computing "the commitment h(k‖I), where k is a secret key and k‖I is the concatenation of k and I. To verify the commitment, the verifying party (in Deng) must have k and I, compute h(k‖I) and compare h(k‖I) with the commitment." The k and I in Deng are not Identity-Based-Encryption (IBE) private keys or secret values. Deng's statement that "the verifying party must have k and I," makes it clear that k and I are not IBE private keys or secret values. Both an IBE private key and a secret value are, by definition, kept secret (private) from recipients (i.e., kept secret from verifying parties).

Because neither Boneh nor Deng shows or suggest using an IBE private key to compute a commitment to a secret value and a corresponding decommitment, claim 1 is patentable over Boneh and Deng even if these references are combined.

Moreover, it was conceded in the Office Action that Boneh "does not disclose using a symmetric key that is based on the IBE private key to encrypt at least one of the commitment and the decommitment." Deng was relied upon as showing this feature. However, Deng does not show or suggest using a symmetric key that is based on the IBE private key to encrypt at least one of the commitment and the decommitment. Col. 6, lines 55-57 of Deng, which was said to be relevant, describes an encrypted message "e(k, m)... containing original message m and a key k using a symmetric key cryptosystem." Col., 6, lines 55-57 of Deng does not relate to the commitment h(k‖I) of Deng (which is not even the same as the commitment of claim 13 as described above). The message m and the key k of Deng, which are encrypted in col. 6, lines 55-57 of Deng, are not commitments or decommitments. For at least these additional reasons, claim 1 is patentable over Boneh and Deng even if these references are combined.

Because neither Boneh nor Deng shows or suggests "using the IBE private key to compute, with computing equipment, a commitment to a secret value and a corresponding decommitment," let alone "using a symmetric key that is based on the IBE private key to encrypt, with computing equipment, at least one of the commitment and the decommitment," claim 13 is patentable over Boneh and Deng whether or not these references

are combined as proposed in the Office Action. Claims 14-17 depend from claim 13 and are allowable because claim 13 is allowable.

Conclusion

The foregoing demonstrates that claims 1-19 are in condition for allowance. Reconsideration and allowance of the application are respectfully requested.

Respectfully submitted,

Date: February 19, 2010

/David C. Kellogg/
David C. Kellogg
Reg. No. 62,958
Agent for Applicant

G. Victor Treyz
Reg. No. 36,294
Attorney for Applicant
Customer No. 36532